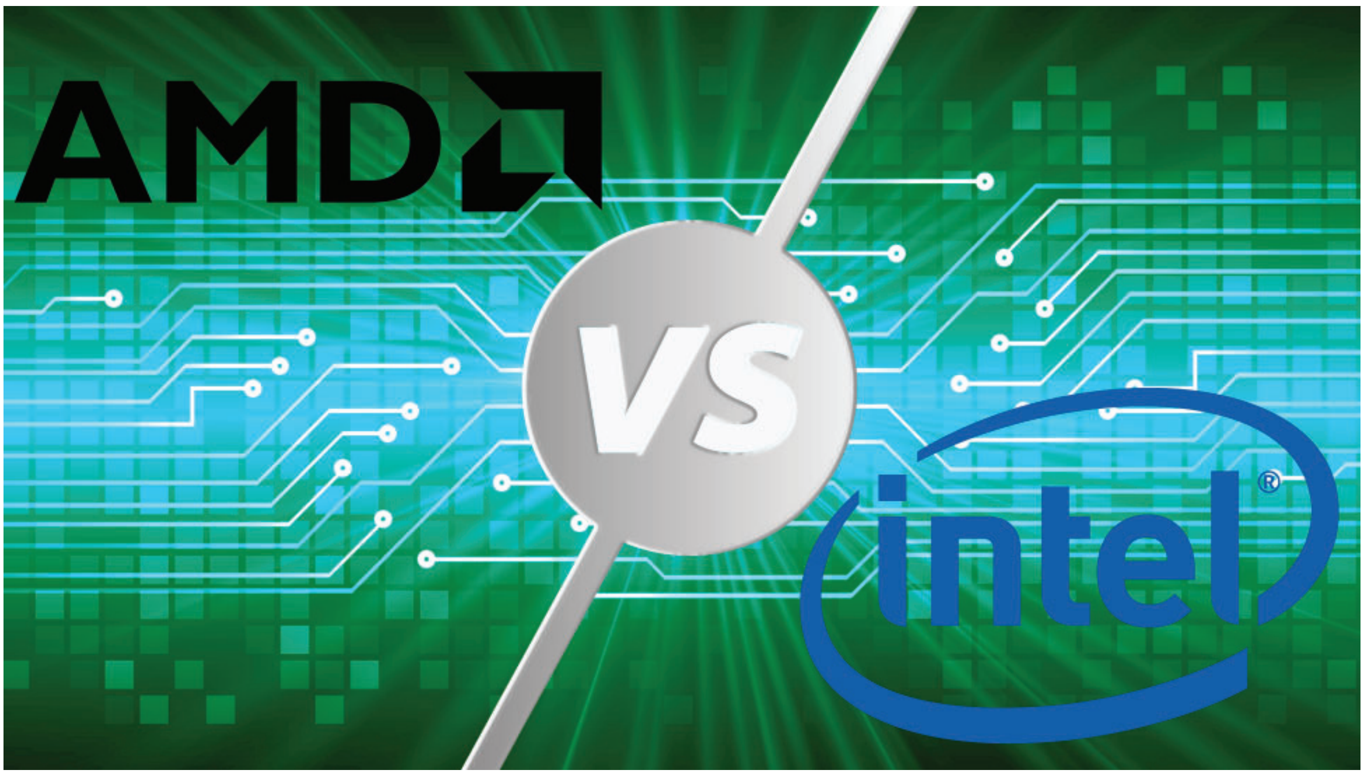
Intel vs AMD Processor Security: Who Makes the Safest CPUs?

By Lucian Armasu November 04, 2019

Who has the most secure processors, AMD or Intel?

Comments (36)

The multi-decade long fight between Intel and AMD has recently taken a new dimension, as more users begin to wonder which processors can protect their computers, data, and online activities best.



(Image credit: Shutterstock)

Up until the last few years, both regular users and cyber security researchers were mostly worried about the plethora of software vulnerabilities for which there never seems to be an end in sight.

However, at the beginning of January 2018, many users and security researchers realized that the hardware powering our devices is not nearly as secure and free from serious security issues as we once thought.

That leaves us with the question: Which company is more secure? The question might seem pedantic when we consider that Intel currently has 242 publicly disclosed vulnerabilities, while AMD has only 16 (a 15:1 difference in AMD's favor), but both companies also have a full roster of special security-minded features.

2018: Year "Zero" In Processor Security

In January 2018, Google's Project Zero security experts, as well as other independent security researchers, disclosed the Meltdown and Spectre CPU design flaws. These vulnerabilities existed because of the design choice most CPU architecture teams have made to

increase the performance of their chips.

The Meltdown flaw, also called Spectre variant 3, affected both Intel and ARM CPUs. It allowed third-party code to break down the isolation between applications and the operating system that is normally enforced by hardware. Attackers can use this to access the memory of other applications and the operating system, thus allowing them to steal secrets.

The Spectre vulnerability breaks the security boundary between different applications, making even those applications that follow best coding practices become vulnerable to attackers that exploit this side-channel security hole in PCs.

Spectre affects virtually all out-of-order CPUs that use speculative execution to increase performance, including AMD and Arm's processors. However, newly discovered side-channel attacks from the Spectre family seem to affect Intel more than the other two vendors, which implies that Intel may have taken more liberties with its CPUs than its competitors to keep the performance edge.

Speculative execution is a CPU design feature that allows a CPU to work on some tasks that may or may not be needed next. If these tasks are needed, then they are more easily accessed when needed, and thus the performance of the CPU increases compared to if this feature didn't exist.

This is also why although specific variants of Spectre can be fixed in software or can even be mitigated in hardware, new variants will keep being discovered by researchers until the CPU makers decide enough is enough and disable the speculative execution feature altogether, or design entirely new architectures.

This isn't just a theory, and it has already happened several times since the original disclosure of the Meltdown and Spectre flaws (in less than two years).

Mere months after researchers revealed Spectre, another group of security researchers prepared to disclose "Spectre Next Generation" family of new speculative-execution flaws. Intel allegedly attempted to delay the disclosure, as the company had already taken a big PR hit earlier that year with the first Spectre reveal.

Speculative execution has created at least two other bugs, Foreshadow and Zombieload, that essentially make Intel's Hyper-Threading technology insecure. OpenBSD founder Theo de Raadt has warned against keeping Hyper-Threading enabled on Intel machines from the start.

It wasn't until the latest Zombieload attack that other OS vendors such as Google and even Apple joined the OpenBSD founder on this. Google disabled Hyper-Threading on all Chromebooks, while Apple noted only that the full mitigation of Zombieload and other Microarchitectural Data Sampling (MDS) vulnerabilities would require disabling Hyper-Threading, leaving it as an option for users.

Intel itself has also recommended disabling Hyper-Threading but only to some customers "who cannot guarantee that trusted software is running on their system(s)." However, with virtually everyone running other people's software on their PCs or servers, who can really tell what's trusted and what isn't?

Attack Surface

The vast majority of speculative execution attacks don't impact AMD's processors, with a few exceptions such as Spectre variants 1, 1.1, and 4, the latter of which is called Speculative Store Bypass.

AMD CPUs were also impacted by PortSmash, a vulnerability affecting its Simultaneous Multi-Threading (SMT) feature, which is similar to Intel's Hyper-Threading. AMD processors were also vulnerable to NetSpectre and SplitSpectre, as these vulnerabilities affected processors, that were also vulnerable to Spectre v1.

AMD's processors were susceptible to Spectre variant 2 and the company issued an update for it, but it said the vulnerability was "difficult to exploit due to our architecture."

AMD's chips were also affected by five out of seven new Meltdown and Spectre attacks found by a group of researchers that included some of the original researchers that discovered the original Spectre and Meltdown design flaws. Intel's chips were susceptible to all seven vulnerabilities.

AMD's CPUs, including the latest Ryzen and Epyc processors, are immune to:

- Meltdown (Spectre v3)
- Spectre v3a
- LazyFPU

- TLBleed
- Spectre v1.2
- L1TF/Foreshadow
- SPOILER
- SpectreRSB
- MDS attacks (ZombieLoad, Fallout, RIDL)
- SWAPGS

As we can see, AMD's CPUs seem to have significantly higher resiliency against speculative execution attacks compared to Intel's processors. However, flaws that are highly similar to Spectre v1 seem to continue to affect AMD's processors, too. The good news is that in most cases, the original Spectre v1 firmware mitigation can also protect against these new flaws.

Both Intel and AMD have issued firmware and software patches for all of the flaws mentioned above although not all of them may have arrived to users if the updating process depended on the motherboard or device makers and not on Intel/AMD, or on the OS vendors such as Microsoft, Apple, etc.

Winner: AMD

Performance Impact Of Spectre Software Mitigations

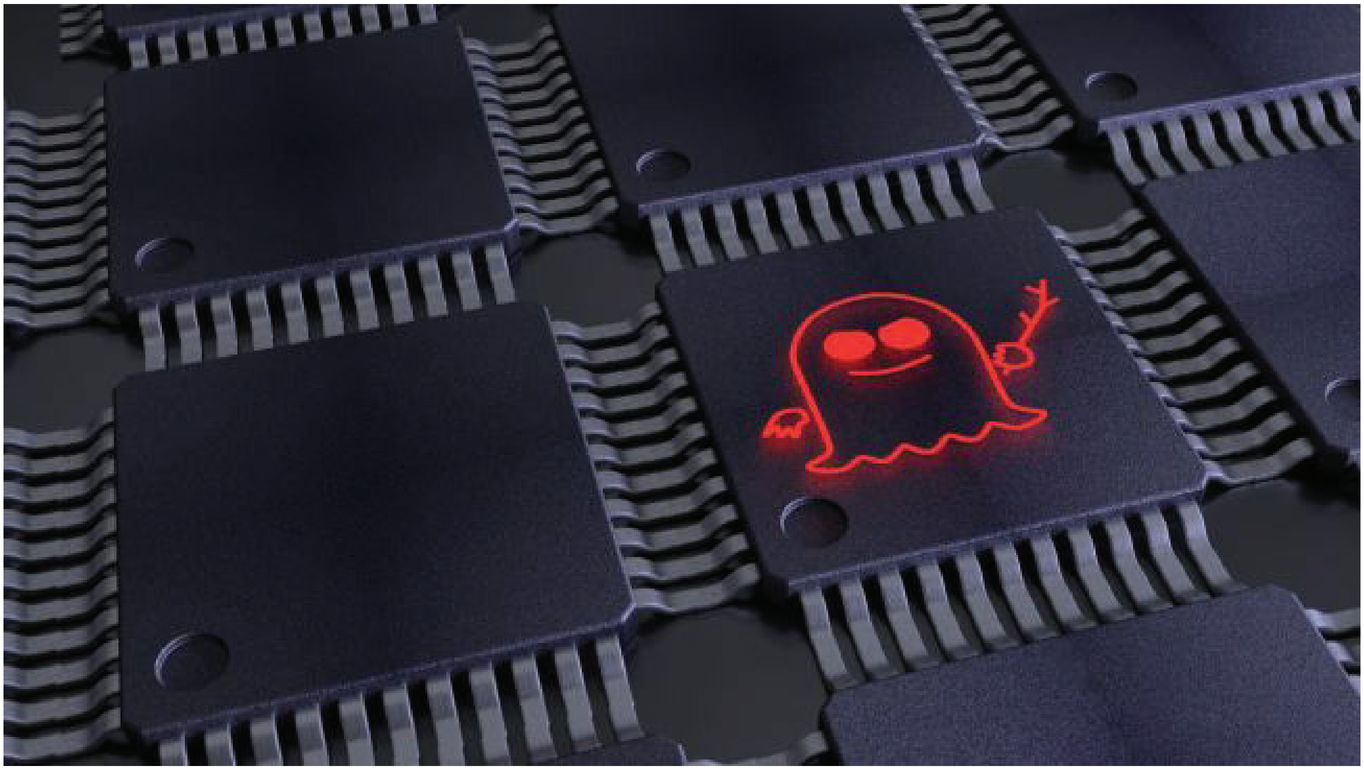
The chipmakers had roughly six months warning about the original Spectre and Meltdown flaws before the public learned about them. This created its own controversy, as not all OS vendors learned about them at the same time. Some were given days or weeks to deal with the bugs.

Even with a six-month head-start, the initial fixes caused quite a few issues on people's computers from significantly slowing down performance to causing them to crash. Things improved somewhat with some updates a few months down the road.

However, even if those patches were optimized to minimize the performance loss, it became quite difficult for the chipmakers -- Intel especially -- to deal with the patching all of the Spectre-class vulnerabilities while still minimizing the performance overhead of the patches.

According to a recent report, all the patches Intel has had to deliver have slowed down users' PCs and servers about five times more than AMD's own patches. That's a significant gap, and it's primarily because Intel has had to fix many more security holes than AMD.

Winner: AMD



(Image credit: Shutterstock)

(Some) Hardware Mitigations Against Side-Channel Attacks

Perhaps because of so many firmware and software mitigations Intel had to issue for Spectre-class security flaws, the company also changed its mind about adding hardware-based mitigations to its processors. Intel was initially somewhat reluctant to do that, or at least to add significant changes to its architecture. However, it later committed to a "security-first" principle.

In some ways, the company has lived up to that commitment. Intel has included hardware mitigations for Meltdown and Foreshadow, as well as partial MDS hardware mitigation in some of its most recent CPUs, starting with select Whiskey Lake and Cascade Lake processors.

The company also promised a hardware fix for Spectre v2 is in the works and has implemented a fix that uses both in-built hardware and software. Intel and AMD haven't fixed Spectre v1, the most dangerous speculation execution attack, in hardware, yet. However, both AMD and Intel have patched Spectre v1 at the software level.

In some cases, Intel has also allegedly ignored, downplayed, or delayed the disclosure of some of the Spectre-class vulnerabilities. In the case of the MDS attacks, Intel allegedly wanted to donate up to $80,000 to the researchers if they downplayed the severity of the MDS attacks. The academics rejected the offer.

It's not clear whether or not Intel is purposefully avoiding fixing Spectre v1 and other side-channel attacks in hardware because it's expensive and it could break too many things, or if the company is just biding time until it's ready to release such a processor.

One thing seems clear, and that is the fact that software patches for speculative execution side-channel attacks will not be enough to prevent similar new attacks from appearing. Academics are skeptical that trying to patch-up the architecture is going to result in long-term security benefits over an architecture design change.

Therefore, if Intel, AMD, and other chipmakers are unwilling to change the design of their CPU architectures, we may be stuck with Spectre-class side-channel attacks forever.

CPU Model and Stepping	V1, Spectre	V2, Spectre	V3, Meltdown	V3a	V4	L1TF, Foreshadow	MFBDS, RIDL	MSBDS, Fallout	MLPDS	MDSUM
Intel64 Family 6 Model 142 Stepping 11	Software	MCU + Software	Hardware	MCU	MCU + Software	Hardware	Hardware	MCU+ Software	MCU+ Software	MCU+ Software
Intel64 Family 6 Model 142 Stepping 12	Software	Hardware + Software	Hardware	MCU	Hardware + Software	Hardware	Hardware	Hardware	Hardware	Hardware
Intel64 Family 6 Model 158 Stepping 11	Software	MCU + Software	Software	MCU	MCU + Software	MCU + Software	MCU+ Software	MCU+ Software	MCU+ Software	MCU+ Software
Intel64 Family 6 Model 158 Stepping 12	Software	MCU + Software	Hardware	MCU	MCU + Software	Hardware	Hardware	MCU+ Software	MCU+ Software	MCU+ Software
R0 Stepping Intel64 Family 6 Model 158 Stepping 13	Software	Hardware + Software	Hardware	MCU	Hardware + Software	Hardware	Hardware	Hardware	Hardware	Hardware
2nd Generation Intel® Xeon® Processors (Formerly Cascade Lake)	Software	Hardware + Software	Hardware	Hardware	Hardware + Software	Hardware	Hardware	Hardware	Hardware	Hardware

(Image credit: Intel - Edited)

There is some movement on patching some vulnerabilities with in-silicon fixes, though. Intel has added new hardware-based mitigations for many of the new vulnerabilities, like MSBDS, Fallout, and Meltdown, with new steppings of its die. Intel is quietly releasing a cadence of new steppings with its 9th-Gen Core processors that add more hardware-boosted mitigation capabilities to already-shipping models. These in-built mitigations are designed to ease the performance overhead of software-based Windows security patches.

Meanwhile, AMD hasn't added any new in-silicon mitigations to its already-shipping chips, though it is working them into newer models. However, it bears mentioning that AMD simply doesn't require as many alterations to fend off vulnerabilities as Intel, so it doesn't require the sheer breadth of hardware-based fixes. As such, we're calling this one in favor of AMD.

Winner: AMD

Intel's ME and Other Security Vulnerabilities

Before the Spectre flaws became known, and even afterward, the biggest privacy or security-related issue with Intel's chips revolved around Intel's built-in Management Engine. However, the speculative execution side-channel flaws overshadowed all the other security vulnerabilities, even though other vulnerabilities may have been just as important.

In 2017, Intel confirmed a security bug in ME that would have allowed attackers to exploit the firmware remotely and take over any Intel-powered machine. The bug affected all processors since 2008.

Later in 2017, researchers found another ME flaw that affected processors from Skylake in 2015 to Coffee Lake in 2017. This one allowed ME to remain active, even if ME could be disabled through unofficial means, as users can't normally disable ME.

Positive Technologies security researchers found a way to disable Intel ME that same year through an undocumented mode that Intel secretly implemented for government authorities. Intel supposedly did this to allow the NSA and other government authorities to disable potentially vulnerable functionality of the ME that would affect everyone else in the PC market.

Researchers also found two new sets of ME security bugs in 2018 while Intel was deep into dealing with the Spectre aftermath.

Due to fears that ME could either be an "official" backdoor or that it could be used like one by malicious parties, some computer makers such as Purism, Systems 76, and even Dell have started offering laptops with ME disabled by default. Google has also started disabling ME for some of its internal devices.

At the time of this writing, there are 242 publicly disclosed Intel firmware vulnerabilities.

AMD's PSP, Ryzenfall, Chimera & Other CPU Flaws

EXHIBIT 6
Page 5 of 17

The AMD Platform Security Processor (PSP), also known as AMD Secure Processor, uses an Arm Cortex-A5 processor to isolate certain chip platform functions from the main processor and the main operating system. It's similar to AMD's ME, and just like ME, it can also be potentially exploited to devastating effect if a malicious party finds a bug in it.

Since 2017, at least three PSP vulnerabilities have been found. A Google security researcher found one in 2017. The bug would have given attackers access to passwords, certificates, and other sensitive information.

Other PSP bugs were found in 2018, along with the disclosure of 13 security flaws in total that affected AMD's Zen-based processors. The researchers placed them into four categories: Ryzenfall, Chimera, Fallout, and Masterkey.

According to the researchers, the Ryzenfall bugs would have allowed attackers to take full control of the AMD Secure Processor. When combined with the bugs classified as Masterkey, the attackers would have also been able to install persistent malware on targets' machines.

The Chimera bugs involved the existence of two manufacturer ASMedia chipset backdoors, one found in the firmware and the other in the hardware (ASIC) of the chipset. The backdoors allowed the injection of malicious code into the Ryzen chipset.

The Fallout flaws allowed attackers to read and write to protected memory areas, such as SRAM and Windows Credential Guard isolated memory.

AMD has mostly downplayed these bugs, saying that in most cases, the attackers would need physical access to the machines to exploit those security vulnerabilities. However, in the CVE Details database we can see that most of them have a very high severity rating:

2	CVE-2018-8936	264	2018-03-22	2018-04-19	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
The AMD EPYC Server, Ryzen, Ryzen Pro, and Ryzen Mobile processor chips allow Platform Security Processor (PSP) privilege escalation.												
3	CVE-2018-8935	264	2018-03-22	2018-04-19	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
The Promontory chipset, as used in AMD Ryzen and Ryzen Pro platforms, has a backdoor in the ASIC, aka CHIMERA-HW.												
4	CVE-2018-8934	264	2018-03-22	2018-04-19	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
The Promontory chipset, as used in AMD Ryzen and Ryzen Pro platforms, has a backdoor in firmware, aka CHIMERA-FW.												
5	CVE-2018-8933	284	2018-03-22	2018-05-09	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
The AMD EPYC Server processor chips have insufficient access control for protected memory regions, aka FALLOUT-1, FALLOUT-2, and FALLOUT-3.												
6	CVE-2018-8932	284	2018-03-22	2018-04-19	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
The AMD Ryzen and Ryzen Pro processor chips have insufficient access control for the Secure Processor, aka RYZENFALL-2, RYZENFALL-3, and RYZENFALL-4.												
7	CVE-2018-8931	284	2018-03-22	2018-04-19	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
The AMD Ryzen, Ryzen Pro, and Ryzen Mobile processor chips have insufficient access control for the Secure Processor, aka RYZENFALL-1.												
8	CVE-2018-8930	20	2018-03-22	2018-05-09	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
The AMD EPYC Server, Ryzen, Ryzen Pro, and Ryzen Mobile processor chips have insufficient enforcement of Hardware Validated Boot, aka MASTERKEY-1, MASTERKEY-2, and MASTERKEY-3.												

(Image credit: Tom's Hardware)

AMD has issued patches to all OEMs and ODMs whose hardware was affected by the bugs, but as usual, it's up to those companies to patch users' computers, which makes support spotty.

Researchers have also found AMD's Secure Encrypted Virtualization (SEV) feature for Epyc server chips to be insecure on occasion. The first SEV vulnerability was announced as part of the Masterkey disclosure mentioned earlier. The researchers said that the Masterkey bugs could be exploited to tamper with the security of SEV as well as that of the firmware Trusted Platform Module (fTPM).

Another group of researchers disclosed a second SEV vulnerability, called SEVered, just a few months later in May 2018. The bug could have allowed attackers to remotely extract memory contents of a virtual machine that would normally be protected by SEV.

A Google researcher found the most recent SEV vulnerability earlier this year. Once again, it involves a bug that allows attackers to extract the encryption keys used by the SEV feature to encrypt the memory contents of the protected VMs.

In other words, this is the third time in about a year that SEV was proven to fail at doing its job -- that of protecting VM memory. This doesn't necessarily put Intel's similar SGX feature in a better position, as it was also found to have several weaknesses caused by the Spectre-family side-channel CPU flaws.

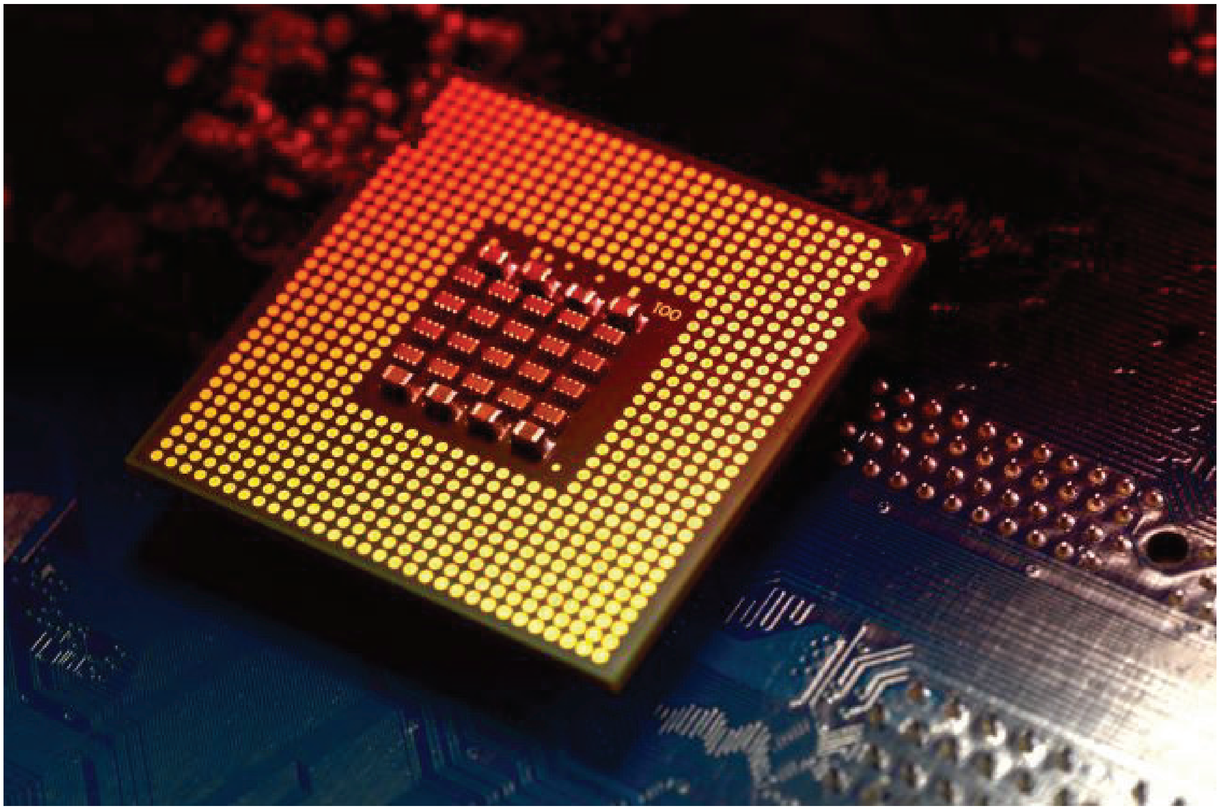
Winner: Tie

Best Intel CPU Security Features

It's not all bad news when it comes to the security of modern processors. Although it is still an emerging initiative, Intel committed to prioritizing security above else after researchers disclosed the first Spectre flaws.

As mentioned earlier, the company has already promised some mitigations for Spectre vulnerabilities in hardware, and a number of them have already landed in current-gen processors.

However, in the end these are just small fixes to something that shouldn't have been broken in the first place, and we're looking for security beyond fixing broken architectures. So what else do Intel processors have to offer in regards to user security?



(Image credit: Shutterstock)

Intel SGX

Software Guard eXtensions is perhaps Intel's most popular and most advanced processor security feature it has released in recent years. SGX enables applications to store sensitive data such as cryptographic keys in a secure virtual enclave inside hardware-encrypted RAM that the main operating system or other third-party applications can't access. Applications such as the end-to-end encrypted Signal messenger make use of it so that it can pair users to each other securely and privately.

Intel TME/MKTME

Intel recently also announced plans to evolve SGX so that it can offer Total Memory Encryption (TME), instead of encrypting only a small portion of memory as SGX does. The new feature is actually two features in one: TME offers a single encryption key for all memory, while another variant called Multi-Key Total Memory Encryption offers -- you guessed it -- full memory encryption with support for multiple keys, such as one key per encrypted VM.

MKTME enables encryption in memory, at rest, as well as in transit. As Intel's feature arrives a little later than AMD's, perhaps the company has learned from its competitor's mistakes with SEV, as well as its own with SGX.

Hardware memory encryption would give users a significant security benefit because it should make it much more difficult for applications to steal data from others in the future (granted the operating systems also put significant restrictions on the APIs that allow apps to share data). However, it's not clear yet whether Intel and AMD intend to leave this feature to enterprise customers or if they'll enable then for mainstream users, too.

Best AMD CPU Security Features

AMD may have been late to the memory encryption game, as Intel beat the company to it with the launch of SGX. However, when AMD launched the Ryzen processors, these came out both with Secure Memory Encryption (SME) and with Secure Encrypted Virtualization (SEV), features that were, and still are, significantly more advanced than Intel's.

AMD SME

The SME feature is typically enabled in the BIOS or other firmware at boot time. It provides page-granular memory encryption support using a single ephemeral 128-bit AES encryption key generated via a hardware random number generator. SME enables applications to mark certain memory pages they use for encryption.

These pages are then automatically encrypted and decrypted when the application needs to read or write that data. The feature protects against physical attacks meant to steal sensitive customer data that still resides in plain-text RAM.

AMD TSME

AMD's Transparent SME is a stricter subset of SME that encrypts all memory by default and doesn't require applications to support it in their own code. It's especially more useful for legacy applications that can no longer be expected to modify their code, but they can still benefit from encryption of the data they process.

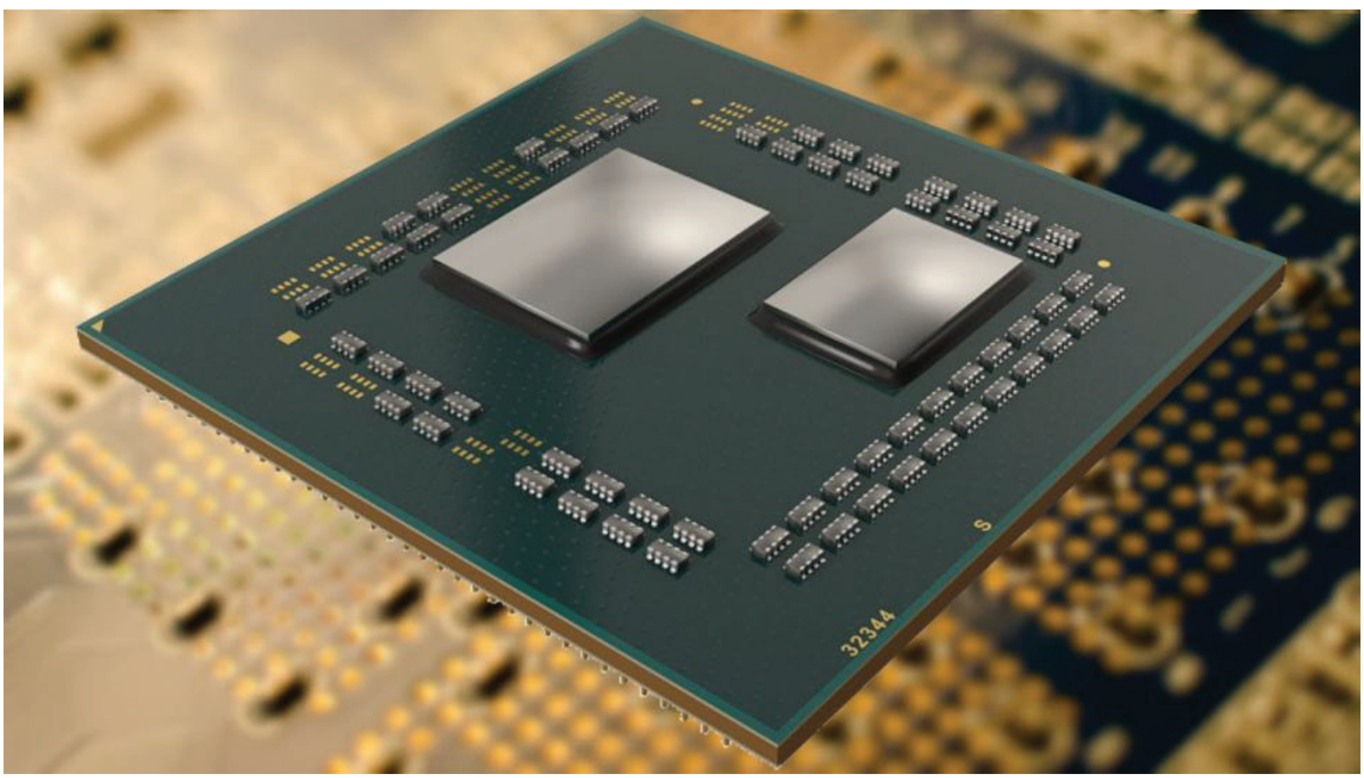
AMD seems to have recently re-branded TSME to "Memory Guard" and included it as part of GuardMI for the company's new Ryzen Pro 3000 CPUs. GuardMI is AMD's alternative to Intel's vPro, which includes both manageability and security features for enterprise customers. One feature AMD has over Intel right now is Memory Guard, which protects a system's data against cold boost attacks.

AMD SEV

AMD's SEV is an extension of SME that encrypts the memory of each VM with its own ephemeral encryption keys. This way, the VMs can stay completely isolated from each other. AMD came up with the idea while working on security features for Sony and Microsoft's consoles.

In practice, SEV, like Intel's SGX, can still prove vulnerable to side-channel attacks or other exploits that gain access to the encryption keys. Both AMD and Intel still have much work to do in terms of ensuring these features are close to invulnerable to attacks.

Winner: AMD



(Image credit: AMD)

EXHIBIT 6
Page 8 of 17

Why Processor Security Matters

Why should you even care about processor security? Aren't the Windows, macOS, or Linux security features enough? The answer is: no, they are not enough, and yes, even you could be affected by these bugs. It's not just data center and web hosting companies that need to worry about these attacks.

First off, the hardware runs at a level below the operating system. Another way of putting it is that the hardware gets to control what the software on top of it ultimately does. Therefore, if anyone takes over hardware, it means they can now control what the operating system and applications do, too. This includes the attackers having control over how those security features work or disabling these features altogether.

Second, even if nobody will attempt to target you by name online, you could still be a victim of a mass-infection of malware that gets spread through advertising networks, hacked sites you visit, internal networks at work, and so on. The hardware exploits could be part of an entire chain of exploitation tools that have on main goal: steal the data of anyone they come across.

If you can't guarantee the security of the hardware in your device, then all the security features of your favorite operating system or applications are basically irrelevant. For instance, this is why Apple and Google have begun building their own servers or have stopped buying from less trustworthy server hardware providers. The two companies implement top-notch security as far as their software goes, but if there is a backdoor in the hardware they use, none of that matters.

Intel vs AMD Processor Security: Conclusion

In the short-to-medium-term, it's probably going to get worse before it gets better for both AMD and Intel's processors, despite the two companies' best efforts. Yes, we'll likely get some more hardware mitigations -- perhaps just enough to appease a large portion of consumers and media, but not quite enough to solve all the issues due to all the difficulties and costs involved in turning major processor architectures around.

We should also get some interesting new security features in the coming years from both Intel and AMD. But the next few years will likely be dominated by more reports of security vulnerabilities found in both the companies' processors as more researchers start digging deeper into their CPU microarchitectures.

It's also going to take the two companies years to fix the flaws the researchers found with new architecture designs. In the end, it should all be for the better as it will force processors to become more mature.

But the question remains, who makes the most secure processors right now that keep you the safest online? We can debate about whether or not researchers took a better look at Intel's flaws because its chips are much more popular, but at the end of the day a few things are undeniable:

1) Intel currently has 242 publicly disclosed vulnerabilities, while AMD has only 16. That's a 15:1 difference in AMD's favor. The gap is just too large to ignore.

2) Less than half of the speculative execution side-channel attacks disclosed for Intel since early 2018 seem to affect AMD's Ryzen and Epyc CPUs. It's true that in some of the cases where the flaws were declared to affect Intel's CPUs, the researchers may not have looked primarily at AMD's CPUs. However, even then AMD confirmed that those bugs didn't affect its processors after carefully verifying how the vulnerabilities affected its own processors. It truly seems as if AMD designed the new Ryzen microarchitecture with better security in mind than Intel's essentially Nehalem-based microarchitectures have been. Why Nehalem-based? Because most of the speculative execution attacks affect Intel's CPUs since at least 2008 when the Nehalem microarchitecture came out.

3) With the release of the new Zen architecture, AMD also seems to have been one step ahead of Intel in terms of supporting new hardware encryption features. It remains to be seen if AMD will maintain this pace in regards to security, as Intel tries to fix all of the Spectre issues and improve its image with consumers, but at least for now, AMD seems to have the lead.

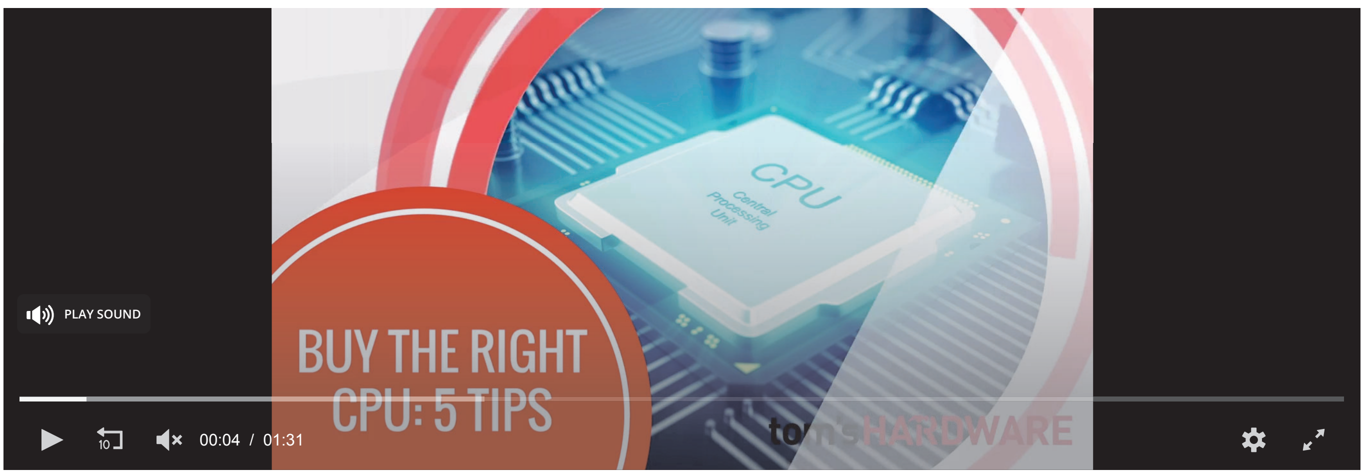
Even ignoring all the various performance slowdowns the Spectre-related patches have caused for both old and new systems alike, AMD's processors seem like the safer and more secure platform to choose in the near and medium-term.

	Intel	AMD
Attack Surface		✗
Performance Impact		✗
Hardware Mitigations		✗
Other CPU Flaws	✗	✗
Best Security Features		✗
Total	1	5

MORE: Best CPUs

MORE: Intel & AMD Processor Hierarchy

MORE: All CPUs Content



MORE ABOUT... | LATEST

Best GPU Benchmarks: How to Test Graphics Cards ▸

The Core i9-10850K Could Cost $450, But We Don't Know If You Can Buy It ▸

SEE MORE RELATED | SEE MORE LATEST ▸

EXHIBIT 6
Page 10 of 17

TOPICS

CPUS SECURITY INTEL AMD

SEE ALL COMMENTS (36)

36 COMMENTS **COMMENT FROM THE FORUMS ▶**

jimmysmitty 04 November 2019 20:26

These are the most useless comparisons. Never a fan when TH does it.

The biggest issue with security vulnerabilities is that just because they are not vulnerable to A doesn't mean there isn't B waiting to be found, or many have been found already just not by someone honest enough to notify anyone of it.

Intel is...

Read More

REPLY ▶

hotaru251 04 November 2019 20:39

> ***jimmysmitty* said:**
>
> These are the most useless comparisons. Never a fan when TH does it.
>
> The biggest issue with security vulnerabilities is that just because they are not vulnerable to A doesn't mean there isn't B waiting to be found, or many have been found already just not by someone honest enough to notify anyone of it.
>
> ...

Read More

REPLY ▶

jimmysmitty 04 November 2019 20:40

> ***hotaru251* said:**
>
> not gonna say it was a good comparison, but undiscovered flaws arent an issue UNTIL they are found.
>
> but even including them the fact is intel's has more at the current time and their "fixes" are more impactful to the end user :/

Majority of fixes tend to only impact HPC operations more than consumers or...

Read More

REPLY ▶

joeblowsmynose 04 November 2019 21:38

Instead of "Winner" ... it should be ... "Less a loser"
"Winning" by having the least vulnerabilities is winning like Charlie Sheen ... ;)

I agree these types of comparisons (by taking some points and declaring a winner/loser) should be left to more fun things like ... CPU cooking, for example.

REPLY ▶

SHOW MORE COMMENTS ▶

MOST POPULAR

The Disco Pixel PC: Building a Flashy, Formidable Mid-Tower in InWin’s 309 Case

By Matt Safford April 29, 2020

READ MORE ▶

Minecraft RTX Performance: You're Going to Need a Beefy GPU

By Jarred Walton April 16, 2020

READ MORE ▶

Gaming Desktop vs. Gaming Laptop: Which Is Better For You?

By Andrew E. Freedman April 11, 2020

READ MORE ▶

Zhaoxin KaiXian x86 CPU Tested: The Rise of China's Chips

By Paul Alcorn April 10, 2020

READ MORE ▶

FreeSync vs. G-Sync 2020: Which Variable Refresh Tech Is Best Today?

By Christian Eberle April 01, 2020

READ MORE ▶

AMD Ryzen Overclocking Guide: Get More from Your CPU

By Jacob Terkelsen April 01, 2020

READ MORE ▶

Retesting The MSI MPG X570 Plus Motherboard

By Thomas Soderstrom March 26, 2020

READ MORE ▶

Doom Eternal Graphics, CPU Testing: id Shows How to Optimize for Performance

By Jarred Walton March 25, 2020

READ MORE ▶

How to Play Doom Eternal on Integrated Graphics

By LowSpecGamer Alex March 24, 2020

READ MORE ▶

The RGBaby: How We Built a Mini ITX RGB Gaming PC

By Andrew E. Freedman March 24, 2020

READ MORE ▶

PlayStation 5 vs. Xbox Series X: Next-Gen Console Face Off

By Jarred Walton March 20, 2020

READ MORE ▶

AMD Radeon RX 5600 XT vs. Nvidia GeForce RTX 2060: Which is the best mainstream GPU?

By Jarred Walton March 17, 2020

READ MORE ▸

Building a $2,000 1440p Gaming PC

By Zak Storey March 13, 2020

READ MORE ▸

BE IN THE KNOW

MOST POPULAR | MOST SHARED

1 Upgrade Your Education: Must-Have Tech for Students 2020

2 Snag 12TB worth of combination external and internal storage for cheap

3 DIY Microscope Uses Raspberry Pi HQ Camera to Take Impressive Photos

4 Sleepy Intel Ice Lake Xeons Take Longer to Ramp Up Frequency Than Expected

5 NVMe Support Likely Coming to Raspberry Pi